In the Drawings:

Amend FIGs. 3A and 4 as indicated in red on the enclosed copies of the drawings as filed.

In the Specification:

Replace the Specification as-filed with the enclosed substitute Specification. A copy of the Specification as-filed, marked up to indicate words being [deleted] or inserted, is also enclosed. No new matter is being introduced.

In the Claims:

For the Examiner's convenience, all of the pending claims as they will stand after this amendment are reproduced below.

1. (Amended) A system for maintaining security in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including

a database for storing a security policy including a plurality of rules; and

a policy distributor, coupled to the database, for distributing the rules through the network;

(2) a security engine, coupled to the network, for storing a set of rules received through the network from the policy distributor and for enforcing the rules with respect to an application; and

(3) an application, coupled to the security engine.

2. (Amended) The system of claim 1, wherein the rules are stored separate from the application.

3. (Amended) The system of claim 1, wherein the security engine further comprises:

an engine for, based on the rules, evaluating a request to access the application; and

an application programming interface (API) for enabling the application and the engine to communicate.

4. The system of claim 3, wherein the security engine further comprises: a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

5. The system of claim 1, further comprising: location means for enabling components in the system to locate each other through the network.

6. The system of claim 1, wherein the policy manager and the policy distributor are hosted on a first server, the security engine and the application are hosted on a second server, and the first and second servers are communicatively coupled to each other through the network.

7. A system for maintaining security for an application in a distributed computing environment, comprising:

an engine, coupled to a network, for storing a set of rules received through the network from a centralized location and for enforcing the rules;

an interface coupled to the engine; and

an application, coupled to the interface to enable the application to communicate with the engine.

8. (Amended) The system of claim 7, wherein the engine stores the rules separate from the application.

9. The system of claim 7, further comprising: a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

10. (Amended) A system for maintaining security in a distributed computing environment, comprising:

(1) a policy manager, coupled to a network, including

a database for storing a security policy including a plurality of rules; and

a policy distributor for distributing the rules through the network;

(2) a plurality of security engines, each coupled to the network, for receiving a set of rules through the network from the policy distributor, storing the set of rules, and enforcing the set of rules; and

(3) a plurality of applications, each application being coupled to a respective security engine, each security engine being able to enforce a set of rules for its respective application.

11. (Amended) The system of claim 10, wherein the security engines store the rules separate from each application.

12. The system of claim 10, wherein each security engine further comprises:

an engine for, based on a set of rules, evaluating a request to access a particular application; and

an application programming interface (API) for enabling a respective application to communicate with a respective engine.

13. The system of claim 12, wherein each security engine further comprises: a plug-in application programming interface (plug-in API) for extending capabilities of the security engine.

14. The system of claim 10, further comprising: location means for enabling components in the system to locate each other through the network.

15. The system of claim 10, wherein the policy manager and the policy distributor are hosted on a policy server, the plurality of security engines and the plurality of applications are hosted on at least one separate server, and the policy server is communicatively coupled through the network to the separate server.

16. A system for maintaining security for a plurality of applications in a distributed computing environment, comprising:

an engine, coupled to a network, for storing a set of rules received through the network from a centralized location, and for enforcing the rules;

a plurality of interfaces coupled to the engine; and

a plurality of applications, each application being coupled to a respective interface to enable the application to communicate with the engine through its respective interface, wherein the engines enforcing the rules for the application.

17. The system of claim 16, wherein the rules are separate from each application.

18. The system of claim 17, further comprising: a plug-in application programming interface (plug-in API) for extending capabilities of the engine.

Cancel claims 19 - 33

Add the following new claims 34 - 35

34. A system for maintaining security in a distributed computing environment, comprising:

a policy manager including a policy database for storing a security policy having a plurality of rules;

zero or more security engines for storing and enforcing a set of rules with respect to an application, said policy manager and said zero or more security engines residing on a single server; and

an application, coupled to the zero or more security engines;

wherein updates to security policies residing on other servers may be synchronized through database replication.

35. A system for maintaining security in a distributed computing environment, comprising:

a policy manager including a policy database for storing a security policy having a plurality of rules;

zero or more security engines for storing and enforcing a set of rules with respect to an application, said policy manager and said zero or more security engines residing on a central server; and

an application, coupled to the zero or more security engines;

wherein other servers storing local security policies may, in response to an authorization request, synchronize local security policy updates with the central server.